UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/470,054	12/22/1999	SUNIL K. SRIVASTAVA	50325-083	5708

29989 7590 02/22/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	13

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/470,054	SRIVASTAVA ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,11 and 13-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,11 and 13-24* is/are rejected.

7)☒ Claim(s) *25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 have been presented for examination. Claims 1-7, 11, and 13 have been amended, claims 8-10 and 12 have been cancelled, and new claims 14-25 have been added in an amendment filed 03/31/2004. Claims 1-7, 11, and 13-25 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) filed on 09/08/2004 was filed after the mailing date of the Notice of Allowance on 06/15/2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement has been considered by the examiner.

Terminal Disclaimer

3. The terminal disclaimer filed on 03/31/2004 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on Application No. 09/407,785 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Prosecution Reopened

4. Prosecution on the merits of this application is reopened on claims 1-7, 11, and 13-24 considered unpatentable for the reasons indicated below.

5. Applicant is advised that the Notice of Allowance mailed 06/15/2004 is vacated. If the issue fee has already been paid, applicant may request a refund or request that the fee be credited

to a deposit account. However, applicant may wait until the application is either found allowable or held abandoned. If allowed, upon receipt of a new Notice of Allowance, applicant may request that the previously submitted issue fee be applied. If abandoned, applicant may request refund or credit to a specified Deposit Account.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-7, 11, and 13-24 are rejected under 35 U.S.C. 102(a) as being anticipated by Sun Microsystems, Inc. (Waldvogel et al.), European Patent Application Publication No. EP 0 952 718 A2.

As per claims 1 and 13, Waldvogel et al. describe a method and computer-readable medium carrying one or more sequences of instructions for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the secure multicast group in a communication network (see ¶ [0038]; figure 1b, items 117 and 111; a key control group linked by any multicast distributes packets with keying material among the plurality of participants in the multicast), wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center (see ¶ [0038]; figure 1b, items 121 and 111; where a sender distributes

the packets containing keying material to receivers; see ¶ [0030]; figure 1a, item 101; where each participant may hold sender and receiver roles), comprising:

creating and storing an original group session key associated with the secure multicast group in a first directory (see ¶ [0042]; figure 1a, item 108; figure 2; item 203; generating a traffic encryption key (TEK) for encrypting messages generated in participant multicast application; see ¶¶ [0049] – [0050]; figure 3, item 401; and holding the current traffic encryption key (TEK) in a group key manager database);

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the secure multicast group, based on the original group session key stored in the first directory (see ¶ [0061]; figure 1b, item 111; a new receiver intending to join the multicast group listens for the heartbeat message resulting in establishing an authenticated connection; see ¶ [0060]; where the heartbeat contains for each key, including the current traffic encryption key (TEK) stored in the group key manager database, the key's ID, version information, and revision information);

receiving a plurality of private keys from the subset of multicast proxy service nodes (see ¶ [0063]; participants providing key encryption keys (KEKs));

receiving a new group session key for the secure multicast group, for use after addition of the first multicast proxy service node (see ¶ [0056]; figure 1a, item 109; communicating to each participant key manager component revised key information in the form of numbers to implement revised keys; see ¶ [0057]; figure 1b, item 118; communicating the changed key from the group manager); from a local multicast proxy service node that has received the original group session key (see ¶ [0059]; figure 1a, items 101 and 108; from a first participant that has the

ad hoc traffic encryption key TEK from the creation of the group); through periodic replication of the first directory (see ¶¶ [0056] – [0057]; periodically changing keying material and revision numbers causing keys to change equivalent to periodic replication of the group key database);

communicating the new group session key to the first multicast proxy service node (see ¶ [0063]; providing the newcomer with the current traffic encryption key (TEK) that has been formed with its entry); and

communicating a message to the subset of the multicast proxy service nodes that causes the subset of the multicast proxy service nodes to update their private keys (see ¶ [0056]; figure 1a, item 101; transmitting a revision number of the key encryption keys (KEKs) to the participants to cause new keying material to be generated for the key encryption keys (KEKs)).

As per claim 2 and 14, Waldvogel et al. further elaborate:

authenticating the first multicast proxy service node based on a second directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes (see ¶ [0061]; figure 1b, items 111 and 120; the new receiver establishes an authenticated connection with an admission control component with an address received from a session directory; see ¶ [0053]; figure 1b, item 120; communicating with the participants to maintain security relationships); and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes(see ¶ [0052]; figure 1b, items 101 and 119; a key manager holding specified information known to a particular participant).

As per claim 3 and 15, Waldvogel et al. then explain:

receiving the new group session key from a node of a second directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes (see ¶ [0056]; figure 1b, item 118; revised keys are implemented by the group key management component; see ¶ [0053]; figure 1b, item 120; communicating with the participants to maintain security relationships) and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes (see ¶ [0056]; figure 1b, item 119; participant key management components causing new keying material to be generated and communicating the increased revision number).

As per claim 4 and 16, Waldvogel et al. also points out:

signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the first directory (see ¶ [0056]; figure 1b, item 119; communicating the increased revision number to the participant key manager component to cause generation of new keying material; see ¶ [0053] ; figure 4; to form a new traffic encryption key (TEK) stored in the database with associated version and revision number).

As per claim 5 and 17, Waldvogel et al. additionally show:

distributing the original group session key to all nodes by creating and storing the original group session key using a first multicast proxy service node of one domain of the first directory (see ¶ [0059]; figure 1a, item 108; creating a traffic encryption key (TEK) as the initial participant creating a key control group as a domain; see ¶¶ [0049] – [0050]; figure 3, item 401; and holding the current traffic encryption key (TEK) in a group key manager database);

replicating the first directory (see ¶¶ [0059] – [0060]; starting a heartbeat announcing itself as the key holder for the traffic encryption key (TEK) just generated with its view of the newest keys in the database); and

obtaining the original group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node (see ¶ [0063], a participant sharing bits in the network address with the newcomer provides the newcomer with the current traffic encryption key (TEK) and key encryption keys (KEKs) of the database).

As per claim 6 and 18, Waldvogel et al. then illustrate:

distributing the new group session key to all nodes by creating and storing the new group session key using a first multicast proxy service node of one domain of the first directory (see ¶ [0056]; figure 1b, item 118; implementing a function to generate revised keys; see ¶ [0053]; figure 4; stored in the database with version and revision numbers);

replicating the first directory (see ¶ [0056]; figure 1b, items 118 and 119; transmitting the revision number to the key manager and each participant key manager component causing new keying material to be generated; see ¶ [0053]; figure 4; stored in a database with version and revision numbers); and

obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node (see ¶ [0057]; figure 1b, item 118; communicating the changed key from the group manager; see ¶ [0053]; figure 4; from the database with version and revision numbers).

As per claim 7, Waldvogel et al. depict a communication system for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the secure multicast group in a communication network (see ¶ [0038]; figure 1b, items 117 and 111; a key control group linked by any multicast distributes packets with keying material among the plurality of participants in the multicast), wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center (see ¶ [0038]; figure 1b, items 121 and 111; where a sender distributes the packets containing keying material to receivers; see ¶ [0030]; figure 1a, item 101; where each participant may hold sender and receiver roles), comprising:

a group controller that creates and manages secure multicast communication among the other multicast proxy service nodes, having a private key (see ¶ [0042]; figure 1a, item 108; figure 2, item 203; a group key management component generating a traffic encryption key (TEK) for encrypting and decrypting messages in the multicast application);

a computer-readable medium comprising instructions which cause:

creating and storing an original group session key associated with the secure multicast group in a first directory (see ¶ [0042]; figure 1a, item 108; figure 2; item 203; generating a traffic encryption key (TEK) for encrypting messages generated in participant multicast application; see ¶¶ [0049] – [0050]; figure 3, item 401; and holding the current traffic encryption key (TEK) in a group key manager database);

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the secure multicast group, based on the original group session key stored in the first directory (see ¶

[0061]; figure 1b, item 111; a new receiver intending to join the multicast group listens for the heartbeat message resulting in establishing an authenticated connection; see ¶ [0060]; where the heartbeat contains for each key, including the current traffic encryption key (TEK) stored in the group key manager database, the key's ID, version information, and revision information);

receiving a plurality of private keys from the subset of multicast proxy service nodes (see ¶ [0063]; participants providing key encryption keys (KEKs));

receiving a new group session key for the secure multicast group, for use after addition of the first multicast proxy service node (see ¶ [0056]; figure 1a, item 109; communicating to each participant key manager component revised key information in the form of numbers to implement revised keys; see ¶ [0057]; figure 1b, item 118; communicating the changed key from the group manager); from a local multicast proxy service node that has received the original group session key (see ¶ [0059]; figure 1a, items 101 and 108; from a first participant that has the ad hoc traffic encryption key TEK from the creation of the group); through periodic replication of the first directory (see ¶¶ [0056] – [0057]; periodically changing keying material and revision numbers causing keys to change equivalent to periodic replication of the group key database);

communicating the new group session key to the first multicast proxy service node (see ¶ [0063]; providing the newcomer with the current traffic encryption key (TEK) that has been formed with its entry); and

communicating a message to the subset of the multicast proxy service nodes that causes the subset of the multicast proxy service nodes to update their private keys (see ¶ [0056]; figure 1a, item 101; transmitting a revision number of the key encryption keys (KEKs) to the participants to cause new keying material to be generated for the key encryption keys (KEKs)).

As per claim 19, Waldvogel et al. further elaborate:

authenticating the first multicast proxy service node based on a second directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes (see ¶ [0061]; figure 1b, items 111 and 120; the new receiver establishes an authenticated connection with an admission control component with an address received from a session directory; see ¶ [0053]; figure 1b, item 120; communicating with the participants to maintain security relationships); and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes(see ¶ [0052]; figure 1b, items 101 and 119; a key manager holding specified information known to a particular participant).

As per claim 20, Waldvogel et al. then explain:

receiving the new group session key from a node of a second directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes (see ¶ [0056]; figure 1b, item 118; revised keys are implemented by the group key management component; see ¶ [0053]; figure 1b, item 120; communicating with the participants to maintain security relationships) and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes (see ¶ [0056]; figure 1b, item 119; participant key management components causing new keying material to be generated and communicating the increased revision number).

As per claim 21, Waldvogel et al. also points out:

signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the first directory (see ¶ [0056]; figure 1b, item 119; communicating the increased revision number to the participant key manager component to cause generation of new keying material; see ¶ [0053] ; figure 4; to form a new traffic encryption key (TEK) stored in the database with associated version and revision number).

As per claim 22, Waldvogel et al. additionally show:

distributing the original group session key to all nodes by creating and storing the original group session key using a first multicast proxy service node of one domain of the first directory (see ¶ [0059]; figure 1a, item 108; creating a traffic encryption key (TEK) as the initial participant creating a key control group as a domain; see ¶¶ [0049] – [0050]; figure 3, item 401; and holding the current traffic encryption key (TEK) in a group key manager database);

replicating the first directory (see ¶¶ [0059] – [0060]; starting a heartbeat announcing itself as the key holder for the traffic encryption key (TEK) just generated with its view of the newest keys in the database); and

obtaining the original group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node (see ¶ [0063], a participant sharing bits in the network address with the newcomer provides the newcomer with the current traffic encryption key (TEK) and key encryption keys (KEKs) of the database).

As per claim 23, Waldvogel et al. then illustrate:

distributing the new group session key to all nodes by creating and storing the new group session key using a first multicast proxy service node of one domain of the first directory (see ¶ [0056]; figure 1b, item 118; implementing a function to generate revised keys; see ¶ [0053]; figure 4; stored in the database with version and revision numbers);

replicating the first directory (see ¶ [0056]; figure 1b, items 118 and 119; transmitting the revision number to the key manager and each participant key manager component causing new keying material to be generated; see ¶ [0053]; figure 4; stored in a database with version and revision numbers); and

obtaining the new group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node (see ¶ [0057]; figure 1b, item 118; communicating the changed key from the group manager; see ¶ [0053]; figure 4; from the database with version and revision numbers).

As per claim 11, Waldvogel et al. describe a communication system for creating a secure multicast or broadcast group, comprising:

a plurality of multicast proxy service nodes having attribute information comprising a group identification value for uniquely identifying a particular node of the multicast proxy service nodes (see ¶ [0048], figure 1a, item 101; each participant is identified with a unique ID such as an address or network identification), and

a directory comprising a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes (see ¶¶ [0053] – [0055]; figure 1a, item 109; figure 3, item 300; keys arranged in a database providing key update messages to participants) and a

replication service agent (RSA) for replicating the attribute information of the one or more multicast proxy service nodes (see ¶ [0056]; figure 1a, item 109; communicating revision numbers to participant key manger components to update the key database);

wherein one of the multicast proxy service nodes generates a first group session key for establishing the secure multicast or broadcast group among the plurality of multicast proxy service nodes (see ¶ [0059]; figure 1a, item 108; figure 1a, item 108; creating a traffic encryption key (TEK) as the initial participant creating a key control group) and

distributes the first group session key to other multicast proxy service nodes in the secure multicast or broadcast group using directory replication (see ¶¶ [0059] – [0060]; starting a heartbeat announcing itself as the key holder for the traffic encryption key (TEK) just generated with its view of the keys in the database; see ¶ [0063]; providing newcomers with the current traffic encryption key (TEK) and key encryption keys (KEKs) of the database).

As per claim 24, Waldvogel et al. further show:

a plurality of client nodes coupled to one of the multicast proxy service nodes,

the one multicast proxy service node creating a secure multicast or broadcast client group that is separate from the secure multicast or broadcast group (see ¶ [0059]; each participant that has recently created a key is a key holder for multicast group different from the multicast group of the key holder emitting a heartbeat superceding its own).

Allowable Subject Matter

8. Claim 25 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. The following is a statement of reasons for the indication of allowable subject matter:

Claim 25 is drawn to a communication system for creating a secure multicast or broadcast group. The closest prior art, Sun Microsystems, Inc. (Waldvogel et al.), European Patent Application Publication No. EP 0 952 718 A2, discloses a similar system. Waldvogel et al. describe the multicast group expanding to joining participants through existing participants with shared bits in the network address with the newcomer (see ¶ [0063]; any participant sharing bits in the network address with the newcomer may provide the newcomer with the current traffic encryption key (TEK) and the key encryption keys (KEKs)). However, they neither teach nor suggest that a plurality of multicast proxy service nodes form a logical arrangement of the plurality of multicast proxy service nodes according to a tree structure, having a root node, one or more intermediate nodes, and one or more leaf nodes. This particular feature explicitly recited in dependent claim 25 renders it to have allowable subject matter.

Conclusion

10. Applicant's submission of an information disclosure statement under 37 CFR 1.97(d) with the fee set forth in 37 CFR 1.17(p) on 09/08/2004 prompted the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 609(B)(2)(a)(ii). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and

statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

January 29, 2005

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100